Safeguarding Privacy Act Data

Privacy Act of 1974, 5 U.S.C. 552a training for DFAS employees, military members, and contractors

Why Take this Training Now

- In a number of recent incidents, personal data has been lost, stolen, or compromised. The most recent theft occurred when a Federal employee took home data on 26.5 million veterans in violation of Department of Veterans Affairs policy.
- The Office of Management and Budget, the Federal entity responsible for overseeing the Privacy Act, has mandated that the Federal workforce complete this training by June 22, 2006.
- Don't YOU or a member of your staff be the next accused of carelessly handling personal data!

Safeguarding Requirements

- Three Levels of Safeguards are Required:
  - ✓ Administrative
  - ✓ Physical
  - ✓ Technical
- These individuals are responsible for establishing safeguards:
  - ✓ Information Technology System Designers
  - ✓ Privacy Act System Managers
  - ✓ Local Privacy Act Officials
- These individuals are responsible for seeing that safeguards are applied:

  YOU!

Marking Privacy Data

- Privacy Act data is to be handled as “For Official Use Only” (FOUO), see DoD 5400.7-R, DoD Freedom of Information Act Program, Chapter 4, located at this Web site: http://www.dtic.mil/whs/directives/corres/html/54007r.htm
- Mark Privacy Act data with a handling notice when it is created or received:
  - ✓ “For Official Use Only – Privacy Act of 1974”; or
  - ✓ “For Official Use Only – Privacy Act Data”
- Place the FOUO marks at the top or bottom of each page or screen. Classified records are marked on both the top and bottom of the page.
- Before disseminating Privacy Act data, make sure it carries the FOUO handling notice.

Transporting Privacy Data

- Using Ground Mail:
  - ✓ Use brown or white envelopes to mail documents.
  - ✓ Never use “holey joes” or messenger-type envelopes.
  - ✓ You may double wrap the documents using an inner and outer envelope if you deem it appropriate.
  - ✓ Mark the envelope to the attention of an authorized recipient.
  - ✓ Never indicate on the outer envelope that the contents contain privacy data.
- Hand-carrying:
  - ✓ When hand-carrying FOUO documents never leave the documents unattended.
  - ✓ Do not leave FOUO documents on a person’s desk, hand them to the recipient to ensure there is no unauthorized access.
- Using E-mail:
  - ✓ Use Common Access Card procedures.
  - ✓ Announce in the opening line of text that you are relaying FOUO material.

Storing Privacy Data

- Duty Hours
  - ✓ Cover or place documents in an out-of-sight location when those not authorized access enter the work space.
  - ✓ Use filtering devices on computer screens to blacken the view.
  - ✓ Lock computers when leaving – even for brief periods.
- After Duty Hours
  - ✓ If the building is locked or manned by security, place records in locked or unlocked drawer or cabinet.
  - ✓ Special categories of privacy data should be placed in locked receptacles.
- What are Some Special Categories of Privacy Data?
  - ✓ Investigative Files
  - ✓ Personnel Files
  - ✓ Security Clearance Files
  - ✓ Adverse Action Files
  - ✓ Any category that, if released, would embarrass or harm the subject.

Disposing of Privacy Data

- Use any means that prevents inadvertent compromise. A disposal method is considered adequate if it renders the information unrecognizable or beyond reconstruction.
- Disposal methods may include:
  - ✓ Tearing, burning, melting, chemical decomposition, pulping, pulverizing, shredding, mutilation.
  - ✓ Recycling contracts are acceptable, if the documents are properly protected while in a destruction bin, protected in transit, and one of the above destruction methods is used by the contractor.

Sharing Privacy Act Data

- Follow the “need-to-know” principle. Share only with those specific DoD employees who need the data to perform official, assigned duties.
- If the Privacy Act System Manager has granted you authority to make disclosures outside DoD:
  - ✓ Share only with those individuals and entities outside DoD that are listed in the “Routine Use” clause of the governing Privacy Act system notice. See this web site for the DoD Privacy Act systems notices:

    http://www.defenselink.mil/privacy/notices/
- If you have doubts about sharing data, consult with your supervisor, the Privacy Act system manager, or your local Privacy Act Officer.

Information for Teleworkers

- Paper Records:
  - ✓ Place Privacy Act data in locked drawers, locked briefcases, or other secure areas where family household members, visitors or intruders cannot access it.
- Electronic Records:
  - ✓ Use password protection protocols. Share your password with no one.
  - ✓ Do not store Privacy Act data on disks, CDs, USB flash drives, memory stick, flashcards, or other media without proper security protections or authorization.
  - ✓ Do not use wireless computer technology without following the proper security protocols.

Reporting Inappropriate Disclosures

- Immediately notify your supervisor, your local Privacy Act Officer, the Privacy Act System Manager, or any other appropriate official of the occurrence.
- For World Wide Web postings, make a note of where the information was posted by copying the Uniform Resource Locator (URL). The URL is the address listed at the top of the screen. Most URLs begin http://www.

Criminal Penalties for Noncompliance with PA

- For knowingly and willfully disclosing Privacy Act data to any person not entitled to access:
  - ✓ Misdemeanor criminal charge, and a fine of up to $5,000 per incident.
- For maintaining a System of Records without meeting the public notice requirements:
  - ✓ Misdemeanor criminal charge, and a fine of up to $5,000.
- For knowingly and willfully requesting or obtaining records under false pretenses:
  - ✓ Misdemeanor criminal charge, and a fine of up to $5,000.

Civil Penalties for Noncompliance with the PA

- The Privacy Act also imposes civil penalties on violators who:
  - ✓ Unlawfully refuse to amend a record.
  - ✓ Unlawfully refuse to grant access to records.
  - ✓ Fail to maintain accurate, relevant, timely and complete data.
  - ✓ Fail to comply with any Privacy Act provision or agency rule that results in an adverse effect.
- Penalties include:
  - ✓ Payment of actual damages.
  - ✓ Payment of reasonable attorney's fees.
  - ✓ Removal from employment.

If You Have Access to Personal Data . . .

- Protect it at all times.
- Do not share it with anyone unless:
  - ✓ The recipient is listed in Section (b) of the Privacy Act or
  - ✓ The record subject has given you written permission to disclose it.
- Password protect personal data placed on shared drives, the Internet or the Intranet.
- Monitor your actions: If I do this, will I increase the risk of unauthorized access?
- **Remember: You may be subject to civil and criminal penalties for violating the Privacy Act.**

More Tips for Avoiding Privacy Breaches

- Take privacy protection seriously.
- Respect the privacy of others.
- Alert your supervisor or other management official when you see personal data left unattended.
- Know the Privacy Act requirements, see DoD 5400.11-R, DoD Privacy Program, for additional guidance. It is located at this Web site:

  http://www.dtic.mil/whs/directives/corres/html/540011.htm

Have questions? Contact the Professionals

- DFAS Freedom of Information Act and Privacy Act Leads:

Linda Krabbenhoft
FOIA/PA Program Manager
DFAS-DCC/DE
(303) 676-6045

Thomas Fasham
FOIA/PA Officer
DFAS-DCC/CL
(216) 522-5225

Larry North
FOIA/PA Officer
DFAS-DCC/IN
(317)510-7365

Dorris Frazier
FOIA/PA Officer
DFAS-DCC/CO
(614) 693-6839

Thank you for completing this important training!